第22卷 第5期
2006年5月

甘肃科技
Gansu Science and Technology

Vol. 22 No. 5
May. 2006

椭圆曲线加密算法的一类实现

曹晓军
(兰州商学院信息工程学院,甘肃 兰州 730020)

摘 要:椭圆曲线密码体制(ECC)是利用椭圆曲线点群上的离散对数问题的难解性而提出的一种公开密钥算法,计算量集中在大数的点乘、点加、模乘、模加、模逆、模幂等方面。本文讨论了椭圆曲线加密算法中涉及的大数计算算法,并用给出椭圆曲线算法的C语言实现。

关键词:椭圆曲线;大数计算;算法
中图分类号:TP301.6

公开密钥算法总是基于一个数学上的难题,比如RSA算法的安全性基于数论中大素数分解的困难性,所以,RSA需采用足够大的整数。因子分解越困难,密码就越难以破译,加密强度就越高。1985年,N. Koblitz和V. Miller分别独立提出了椭圆曲线密码体制(ECC),其依据就是定义在椭圆曲线点群上的离散对数问题的难解性。

1 椭圆曲线加密算法

1.1 椭圆曲线基本协议

设椭圆曲线为E(Fq),在加法群中的阶为n,我们设点P0(1,1)为该椭圆曲线上的点,A和B为进行通信的双方用户。该椭圆曲线上的消息加密及解密协议如下:设素数p和q满足q=p;A的公钥为点Pa=ka×P0,私钥为ka;B的公钥为点Pb=kb×P0,私钥为kb;m为消息。

(1)随机产生k,计算(x,y)=k×Pb;计算R=k×P0;计算c=m×x(mod p);发送密文(R,c)->b。

(2)计算(x,y)=kb×R;计算m=c÷x(mod p),m即为经由解密得到的明文。

1.2 椭圆曲线密码体制中的有关计算

作为公开密钥算法的一种,椭圆曲线密码体制要用到点乘、点加、模乘、模加、模逆、模幂这些基本运算,点加和点乘属于椭圆曲线群上的运算,它们的执行速度直接决定着椭圆曲线的加密速度。为了提高速度,可从采用高速算法或实现并行性两方面解决。

2 大数计算的典型算法

对于大数,本文关心的是整型数据类型,因此仅对整型数据类型部分展开讨论。

2.1 大数的常规运算的实现

对于加减法运算,通过将A、B按位对齐;低位开始逐位相加(减);对结果做进进(借)位调整即可实现。乘法运算引入sum2、sum1作为中间量;在n的每一位上处理m;通过每一层循环,实现乘法的加法化;对结果做进借位调整。出发运算则要引入al来标识a的长度,bl来标识b的长度;测算a和b的长度;从高位开始,对位做减法,并完成借位;然后高位开始逐位计算商并整理商,产生余数。余数也可作为取模的结果。

2.2 大数模乘算法

大数模乘算法在密码学领域有广泛的应用,它是公钥密码的基本运算。模乘一般表示为:C=(A B)mod N,0≤A,B<N,其中A、B、N都为k比特二进制大整数。以下是目前具有代表性的几种大数模乘算法:

Blakley的加法型模乘算法,将模乘转换为一系列加法。算法每次计算都对累加中间结果C进行模简化,以使结果小于N。Blakley算法不含乘法和除法,但加法法和模简化过程只能逐位处理,实现效率不够理想。针对Blakley算法,人们相继提出了不少改进方法,这些改进主要可分为二大类:减少乘法过程的加法次数,即减少乘数中非0个数;提高模简化速度等。F. E. Su和T. H. Wang于1996年提出了一种无需大数比较而直接将C限制在 范围内

的模简化方法，明显提高了效率。围绕减少加法次数，Koc利用窗口技术，通过以m位为一组结合冗余二进制数方法从右到左对乘数重编码和预计算，提出了窗口模乘算法。不久又出现了有符号滑动窗口模乘算法和无符号滑动窗口模乘算法，也是目前较为理想的加法型模乘算法。

为避免商计算中的除法运算，Pope和Stein提出了一种采用估商技术的模简化思想，Knuth利用该思想给出了一种具体的估商型模乘算法。Knuth算法的优点是将商计算转化为一个25位数与t位数的除法，由于算法中仍含除法，实现效率受影响较大。1987年Barrett提出了第一种无除法的估商型模乘算法，其基本思想是用乘法和预计算替代除法。Barrett算法的最大优点在于整个计算不含除法，仅用最基本的字乘和字加即可完成。1992年Quisquater提出了另一种估商型模乘算法，其特点是可快速进行商计算，后来Walter亦提出了类似的思想。Quisquater算法进一步简化了估商计算，但整个模幂过程中需附加一次归范化和反归范化计算。

1985年Montgomery借助一个新的特殊剩余系，将普通模乘转换为易计算的特殊模乘，提出了一种模乘的有效算法：采用模加右移法，避免了公钥加密中求模算法的除法运算，使运算量大为减少。Montgomery算法不含除法，基本运算为字乘和字加，通过剩余系转换方法计算模乘，极大地提高了模乘计算速度，被广泛应用于各种软硬件实现中，人们也从高效率、低空间、高安全等角度对算法进行了各种改进。Montgomery型算法最后都需对作一次条件减法，由于不同乘数所耗费的时间和能量不同，给时间攻击、能量攻击及电磁攻击留下了余地，为此Walter、Hachez和Quisquater通过深入研究，提出了一种可有效阻止这些攻击的Montgomery型无减法模乘算法，而且实现效率也相当理想。

2.3 大数分解问题

大数分解问题涉及到高可信度的计算问题及很多数学技术的进一步研究和运用，包括信息论，竞争的复杂性等。数论学者和计算机学者已经得到了许多实际有效的方法并已经引起人们的普遍关注。

大数分解质因子问题涉及到了素数判别和大数分解两方面的内容。而进行素数判别和大数分解最直接的方法就是试除法，即对于整数n来说，用2，…，n－1去试除，然后判定n是否素数，分解式是什么。作为最简单的一个方法，试除法对较大的数(20位左右)进行分解是要耗费很多时间。费马方法给定n，若n是两数平方差n＝a2－b2，则n＝(a＋b)(a－b)是n的一个因子分解，但该方法只有当n有两个几乎相等的因子时，才比较快。勒让德方法将分解奇数n的问题，转化为寻找形如x2≡a2(mod n)的同余式的非平凡解问题。勒让德方法的困难之处正是如何寻找同余式的非平凡解。直到1931年，勒默和鲍尔斯首次用连分数解决了这个困难。1975年，莫利桑和卜利尔哈特，对勒默的方法作了深入的研究，将其发展成为一个较系统的好算法，连分数法就被人们广泛应用于分解因子。到目前为止，它被认为是最有力的分解工具之一，而用它也可以方便地在计算机上分解50位左右的数。

3 椭圆曲线加密的实现

```
encryptogram( ) //加密
{
int i;time_t t;
  srand( (unsigned) time( &t ) );
  rando(p2);
  int product[301],quo[301],arith[201];
  for(i=1;i<301;i++)
  product[i]=0;
multiply(p1,p2,product);
rando(p3);
division(product,p3,quo,arith);
int p4[101],prod[301];
random(p4);
for(i=1;i<301;i++)
prod[i]=0;
multiply(p4,arith,prod);
}
decryptogram( ) //解密
{
int pro[301],qu[301],arit[201],q[301],ari
[201];
for(i=1;i<301;i++)
pro[i]=0;
multiply(p1,p2,pro);
division(pro,p3,qu,arit)
division(prod,arit,q,ari);
return 0;}
```

参考文献：

〔1〕 王永祥.超高精度大数算法与程序设计〔M〕.陕西：西安交通大学出版社.1990.6

(下转第94页)

如图所示，Digital Clock Manger (DCM) 产生时钟和它的倒相时钟。这种产生时钟的方法有两个优点：

(1)所有的数据，控制和时钟信号在输入 FPGA 时都要经过相似的延迟部件。

(2)当全局时钟线网被用作时钟和 180°相移时钟的时候，时钟占空比失真度最小。

所有的地址和控制信号在 IOB 中寄存和输出。地址和控制信号使用的是存储器时钟的 180°相移时钟。这样的方法使得地址和控制信号在被寄存之前可以有额外的富余时间；地址和控制信号可以容易的与要求的时序一致。

3 与其他数据捕获技术的比较

3.1 印制板布线延时接收技术

这种技术是利用增减印制板上的走线长度来控制数据延时。由于从存储器读出的数据和数据选通信号是边缘对齐的，所以可以通过走线长度来增加数据选通信号的延时，并将延时后的数据选通信号作为接收数据的打入时钟，走线的长度可以通过对相关参数的估算大致得出。这种方法的优点是相对简单，控制器中不需要再增加额外的延时逻辑，但是缺点也很明显，就是延时固定，不能随着频率、温度和电压等因素的波动而变化，因此，该方法仅适用于工作频率不太高的简单系统中，并不适用于高速的 DDR 存储控制器。

3.2 核心时钟移相接收技术

该技术的核心思想是利用调整存储控制器的核心时钟相位，产生一个全局性的时钟，通过这个全局时钟来同时接收所有的读出数据。在电路逻辑设计中，常用的方法是利用锁相环技术对时钟相位进行调整。这种技术的优点在于控制电路比较简单，省去了数据缓冲器，但是也存在很大的缺点，主要表现在两个方面：一方面是所有的数据都同时接收，这样数据的有效窗口就较小；第二个方面是由于接收时钟身兼二职，既要负责接收数据，又要考虑和核心时钟之间的同步，使得难以选择和控制接收时钟的相位。所以这种方法主要用于工作频率较低的系统中。

4 总结

本文就一种 DDR SDRAM 存储控制器设计中使用的数据捕获技术进行了详细分析，并对各种技术的优劣进行了比较。不同的接收技术，需要和依赖不同类型的硬件资源。针对不同的环境和系统，根据硬件资源的实际情况，所采用的数据捕获技术也不相同。在用 FPGA 实现进行验证过程中，FPGA 器件所提供的硬件资源，如精细可调的延时单元、高性能的双端口存储器、可精确控制相位的时钟锁相环、高速低延时的布线资源等，都决定了该采用何种数据接收技术。半导体工艺的发展非常快速，这必然有助于存储控制器设计采用新的数据接收技术，以最大限度地提高存储系统的性能，满足日益增长的高性能计算需求。

(上接第 96 页)

〔2〕 朱文余 孙琦. 计算机密码应用基础〔M〕. 北京：科学出版社. 2003.8

〔3〕 求是科技 谭思亮. 监听与隐藏——网络侦听揭密与数据保护技术〔M〕. 北京：人民邮电出版社. 2002.8

〔4〕 阙喜戎 孙锐 等. 信息安全原理及应用〔M〕. 北京：清华大学出版社. 2003.7

〔5〕 (美)Harold F. Tipton Micki Krause 著 王卫卫 杨波等译. 信息安全管理手册〔M〕. 北京：电子工业出版社. 2004.6

〔6〕 王昌锐. 大数论〔M〕. 台北：徐氏基金会. 1970

〔7〕 杨君辉 等. 一种椭圆曲线签名方案与基于身份的签名协议〔J〕. 软件学报. 2000.7－12

〔8〕 陈克非 李祥. 密码学进展－CHINACRYPT'2004 第八届中国密码学学术会议论文集〔C〕. 北京：科学出版社. 2004.4

〔9〕 王金荣 等. 大数模乘算法的分析与研究〔J〕. 计算机工程与应用. 2004.24

〔10〕 陈昭智 郑建德. Montgomery 算法在大数模幂运算中的改进〔J〕. 厦门大学学报(自然科学版). 2004.8

〔11〕 沈丽敏 等. 特征为 3 的域上的椭圆曲线点的快速计算〔J〕. 数学杂志. 2004 年第 24 卷

〔12〕 任铁良 等. 大数组在 C＋＋中的实现及应用〔A〕. 1999.4